Next 2 Page(s) In Document Exempt

Approved For Release 2003/08/13 : CIA-RDP84B00890R000300020010-4

General Services Administration
Information Security Oversight Office
Washington, DC 20405

ER 81-5384

OCT 16 1981

XI-C300/12

Honorable William J. Casey
Director
Central Intelligence Agency
Washington, DC 20505

Dear Mr. Casey:

The Honorable Richard V. Allen, Assistant to the President for National Security Affairs, has requested that I coordinate the executive branch review of Executive Order 12065, "National Security Information," for purposes of recommending to the President a revised information security system that reflects the policies of the Administration. In keeping with Mr. Allen's instructions, I enclose for your review and comment a draft of a proposed new executive order. Please submit your comments to me no later than November 16, 1981.

The enclosed draft is largely based upon a proposed executive order which a committee composed of representatives of the intelligence community recently submitted to Mr. Allen. The Information Security Oversight Office (ISOO) has revised this proposal based upon its efforts to incorporate, if merited, changes to E.O. 12065 suggested by executive branch agencies in response to an earlier solicitation by this office, as well as ISOO's own oversight experience in this area. ISOO has coordinated this redraft with the National Security Council staff and representatives of the intelligence community committee which produced the initial draft. While there are points of disagreement within the executive branch on certain issues, there is a general consensus that these preliminary efforts have produced a draft which will facilitate the preparation of a final version to be presented to the President as quickly as possible. With that goal in mind, I do not anticipate transmitting any later draft for general comment.

You are invited to send a representative to a question and answer meeting I will convene on Tuesday, October 27, 1981, from 1:30 to 4:30 p.m., in Room 5141A, General Services Administration Building, Eighteenth and E Street entrance. Please direct your questions to me at 633-6880. Your cooperation in preventing the unnecessary dissemination of this draft is appreciated.

Sincerely,

(Signed) Steven Garfinkel

STEVEN GARFINKEL
Director

Enclosure

cc: Mr. Harry E. Fitzwater
Deputy Director for Administration

Executive Order _____

National Security Information

The interests of the United States and its citizens require that certain information concerning our national defense and foreign relations be protected against unauthorized disclosure. It also is essential that the public be informed concerning the activities of its Government. This Order prescribes a uniform information security system for classifying, declassifying and safeguarding national security information. It also establishes a monitoring system to ensure its effectiveness. Nothing in this Order shall limit the protection afforded any information by other provisions of law.

SECTION 1. ORIGINAL CLASSIFICATION.

1-1. Classification Levels.

1-101. National security information that requires protection against unauthorized disclosure (hereinafter "classified information") shall be classified at one of the following three levels:

(a) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

(b) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

(c) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

1-102. Except as otherwise provided by statute, no other terms shall be used to identify classified information.

1-103. If there is reasonable doubt about the need to classify information, the information shall be considered classified and shall be safeguarded under the provisions of this Order pending a final determination by an original classification authority.

1-2. Classification Authority.

1-201. Top Secret. The authority to classify information originally as Top Secret may be exercised only by:

(a) The President;

(b) agency heads and officials as designated by the President in the Federal Register; and

(c) officials delegated this authority under Section 1-204.

1-202. Secret. The authority to classify information originally as Secret may be exercised only by:

(a) Agency heads and officials as designated by the President in the Federal Register;

(b) officials with original Top Secret classification authority; and

(c) officials delegated such authority pursuant to Section 1-204.

1-203. Confidential. The authority to classify information originally as Confidential may be exercised only by:

(a) Agency heads and officials as designated by the President in the Federal Register;

(b) officials with original Top Secret or Secret classification authority; and

(c) officials delegated such authority pursuant to Section 1-204.

1-204. Delegation of Original Classification Authority.

(a) Delegations of original classification authority shall be limited to the minimum required to administer this Order. Agency heads are responsible for ensuring that subordinate officials so designated have a demonstrable and continuing need to exercise this authority.

(b) Original Top Secret classification authority may be delegated only by the President; an agency head or official designated pursuant to Section 1-201(b); and the senior official designated under Section 5-301(a), provided that official has been delegated original Top Secret classification authority by the agency head.

(c) Original Secret classification authority may be delegated only by the President; an agency head or official designated pursuant to Sections 1-201(b)

and 1-202(a); an official with original Top Secret classification authority; and the senior official designated under Section 5-301(a), provided that official has been delegated original Secret classification authority by the agency heads.

(d) Original Confidential classification authority may be delegated only by the President; an agency head or official designated pursuant to Sections 1-201(b), 1-202(a), and 1-203(a); an official with original Top Secret classification authority; and the senior official designated under Section 5-301(a), provided that official has been delegated original Secret or Confidential classification authority by the agency head.

(e) Each delegation of original classification authority shall be in writing. It shall identify the authority by name or position title.

1-205. Exceptional Cases. When an employee, contractor, or grantee of an agency that does not have original classification authority originates information believed by the employee, contractor, or grantee to require classification, the information shall be protected in a manner consistent with this Order and its implementing directives. The information shall be transmitted promptly

under adequate safeguards to the agency which has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within thirty (30) days whether to classify this information. If it is not clear which agency has classification responsibility for this information, it shall be sent to the Director of the Information Security Oversight Office. The Director shall consult with the agency determined to have primary subject matter interest in this information before making a classification determination.

I-3. Classification Categories.

I-301. Information shall be considered for classification if it concerns:

(a) military plans, weapons, or operations;

(b) the vulnerabilities or capabilities of systems, installations, projects, or plans vital to the national security;

(c) foreign government information;

(d) intelligence activities (including special activities), or intelligence sources or methods;

(e) foreign relations or foreign activities of the United States;

(f) scientific, technological, or economic matters relating to the national security;

(g) United States Government programs for safeguarding nuclear materials or facilities;

(h) cryptology;

(i) a confidential source; or

(j) other categories of information which are related to the national security and which require protection against unauthorized disclosure as determined by the President or by agency heads who have original classification authority. Any determination made under this subsection shall be reported promptly to the Director of the Information Security Oversight Office.

I-302. Information which is determined to concern one or more of the categories in Section I-301 shall be classified when an original classification authority also determines that its unauthorized disclosure reasonably could be expected to cause damage to the national security. In considering whether the disclosure of

information could be expected to cause damage to the national security, information shall be classified if its unauthorized disclosure, when considered in the context of related information, reasonably could be expected to cause such damage.

1-303. Unauthorized disclosure of foreign government information, or information relating to intelligence sources or methods is presumed to cause damage to the national security.

1-304. Information classified in accordance with Section 1-3 shall not be declassified automatically as a result of any unofficial publication or inadvertent or unauthorized disclosure in the United States or abroad of identical or similar information.

1-4. Duration of Classification.

1-401. Information shall be classified for as long as required by national security considerations. If appropriate, the original classification authority shall set a specific date or event for declassification at the time the information is originally classified.

I-402. Automatic declassification determinations under predecessor orders shall remain valid unless extended by an authorized official of the originating agency. These determinations may be by individual documents or categories of information. The agency shall be responsible for notifying holders of the information of such determinations.

I-403. Information classified under predecessor orders and marked for declassification review shall remain classified until reviewed for declassification under the provisions of this Order.

I-5 Identification and Markings.

I-501. At the time of original classification, the following shall be shown on the face of all classified documents, and prominently displayed, where practicable, on all other forms of classified information:

(a) The identity of the original classification authority if other than the person whose name appears as the approving or signing official (unless this information itself would reveal a confidential source or relationship not otherwise evident in the document or information);

(b) the agency and office of origin (unless this information itself would reveal a confidential source or relationship not otherwise evident in the document or information);

(c) the date or event for declassification, or the notation "Originating Agency Review Required"; and

(d) one of the three classification levels defined in Section 1-1.

1-502. Marking designations implementing the provisions of this Order, including abbreviations, shall conform to the standards prescribed in implementing directives issued by the Information Security Oversight Office.

1-503. Foreign government information shall either retain its original classification or be assigned a United States classification that shall ensure a degree of protection at least equivalent to that required by the entity that furnished the information.

1-6. Limitations on Classification.

1-601. Classification shall be determined solely on the basis of national security considerations. In no case shall information be classified in order to conceal

violations of law, inefficiency or administrative error; to prevent embarrassment to a person, organization or agency; to restrain competition; or to prevent or delay the release of information which does not require protection in the interest of national security.

1-602. The President or an agency head or official as provided in Sections 1-201(b), 1-202(a) or 1-203(a) may re-classify information previously declassified and disclosed if it is determined in writing that (a) the information requires protection in the interest of national security; and (b) the information may reasonably be recovered.

1-603. Information may be classified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), or the Mandatory Review provisions of this Order (Section 3-4) if such classification meets the requirements of this Order and is accomplished personally and on a document-by-document basis by the agency head, the deputy agency head, the senior agency official designated under Section 5-301(a), or an official with original Top Secret classification authority.

SECTION 2. DERIVATIVE CLASSIFICATION.

2-1. Use of Derivative Classification.

2-101. Derivative classification is the determination that information is in substance the same as information currently classified, and the application of the same classification markings. Persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority.

2-102. Persons who apply derivative classification markings shall:

(a) Observe and respect original classification decisions; and

(b) carry forward to any newly created documents any assigned authorized markings. The most restrictive declassification date or event shall be used for documents classified on the basis of multiple sources.

2-2. Classification Guides.

2-201. Agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative classification of information.

2-202. Each guide shall be approved personally and in writing by an official who:

(a) Has program or supervisory responsibility over the information or is the senior agency official designated under Section 5-301(a); and

(b) is authorized to classify information originally at the highest level of classification prescribed in the guide.

2-203. Agency heads may, for good cause, grant and revoke waivers of the requirement to prepare classification guides for specified classes of documents or information. The Director of the Information Security Oversight Office shall be notified of any waivers.

SECTION 3. DECLASSIFICATION AND DOWNGRADING.

3-1. Declassification Authority.

3-101. Information shall be declassified or downgraded as soon as national security considerations permit. Agencies shall coordinate their review of classified information with other agencies that have a direct interest in the subject matter. Information that continues to meet the classification requirements prescribed by Section 1-3 despite the passage of time will continue to be protected in accordance with this Order.

3-102. Information shall be declassified or downgraded by the official who authorized the original classification, if that official is still serving in the same position; the originator's successor; a supervisory official of either; or officials delegated such authority in writing by the agency head or the senior agency official designated pursuant to Section 5-301(a).

3-103. If the Director of the Information Security Oversight Office determines that information is classified in violation of this Order, the Director may require the information to be declassified by the agency that originated the classification. Any such decision by the Director may be appealed to the National Security

Council. The information shall remain classified until the appeal is decided.

3-104. The provisions of this section shall apply to agencies which, under the terms of this Order, do not have original classification authority, but which had such authority under predecessor orders.

3-2 Transferred Information.

3-201. In the case of classified information transferred in conjunction with a transfer of functions, and not merely for storage purposes, the receiving agency shall be deemed to be the originating agency for purposes of this Order.

3-202. In the case of classified information which is not officially transferred as described in Section 3-201, but which originated in an agency which has ceased to exist and for which there is no successor agency, each agency in possession of such information shall be deemed to be the originating agency for purposes of this Order. Such information may be declassified or downgraded by the agency in possession after consultation with any other agency which has an interest in the subject matter of the information.

3-3. Systematic Review for Declassification

3-301. The Archivist of the United States shall, consistent with procedures prescribed in the Information Security Oversight Office's directives implementing this Order, systematically review for declassification (i) classified records accessioned into the National Archives of the United States, and (ii) classified presidential papers or records in the Archivist's possession and control. Such information shall be reviewed by the Archivist for declassification in accordance with systematic review guidelines that shall be provided by agency heads who originated the information, or in the case of foreign government information, by the Director of the Information Security Oversight Office, in consultation with interested agency heads. The Secretary of Defense may establish special procedures for systematic review for declassification of classified cryptologic information, and the Director of Central Intelligence may establish special procedures for systematic review for declassification of classified information pertaining to intelligence activities, (including special activities), or intelligence sources and methods.

3-302. Agency heads may conduct internal systematic review programs for classified information originated by their agencies contained in permanently valuable records

which have not been accessioned into the National Archives of the United States.

3-4. Mandatory Review for Declassification.

3-401. Except as provided in Section 3-402, all information classified under this Order or predecessor orders shall be subject to a review for declassification by the originating agency, if:

(a) the request is made by a United States citizen or permanent resident alien, or a State or local government; and

(b) the request describes the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort.

3-402. Information less than twelve years old originated by the President, the White House Staff, by committees or commissions appointed by the President, or others acting on behalf of the President, including such information in the possession and control of the Administrator of General Services pursuant to sections 2107, 2107 note, or 2203 of title 44, United States Code, is exempted from the provisions of Section 3-401. Such information over twelve years old shall be subject to mandatory review for

declassification in accordance with the provisions of this Section.

3-403. Agencies conducting a mandatory review for declassification shall declassify information no longer requiring protection under this Order. They shall release this information unless withholding is otherwise appropriate under applicable law.

3-404. Agency heads shall develop procedures to process requests for the mandatory review of classified information. These procedures shall apply to information classified under this or predecessor orders. They shall also provide a means for administratively appealing a denial of a mandatory review request. The Secretary of Defense shall develop special procedures for the review of cryptologic information, and the Director of Central Intelligence shall develop special procedures for the review of information pertaining to intelligence activities (including special activities), or intelligence sources or methods, after consultation with affected agencies. The Archivist shall develop special procedures for the review of information accessioned into the National Archives of the United States. All procedures for mandatory review shall be reviewed by the Director, Information Security Oversight Office, to ensure that they

are consistent with this Order and its implementing directives.

3-405. In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974, or the Mandatory Review provisions of this Order:

(a) An agency shall refuse to confirm or deny the existence or non-existence of requested information whenever the fact of its existence or non-existence is itself classifiable under this Order.

(b) When an agency receives any request for documents in its custody that were classified by another agency, it shall refer copies of the request and the requested documents to the originating agency for processing, and may, after consultation with the originating agency, inform the requester of the referral. In cases in which the originating agency determines in writing that a response under Section 3-405(a) is required, the referring agency shall respond to the requester consistent with that Section.

SECTION 4. SAFEGUARDING.

4-1. General Restrictions on Access.

4-101. A person is eligible for access to classified information only after a formal determination of trustworthiness has been reached by agency heads or designated senior officials and provided that such access is essential to the accomplishment of authorized and lawful Government purposes.

4-102. Controls shall be established by each agency to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed only under conditions that will provide adequate protection and prevent access by unauthorized persons.

4-103. Classified information shall not be disseminated outside the executive branch except under conditions which ensure that the information will be given protection equivalent to that afforded within the executive branch.

4-104. Except as provided by directives issued by the President through the National Security Council, classified information originating in one agency may not be disseminated outside any other agency to which it has

been made available without the consent of the originating agency.

4-2. Special Access Programs.

4-201. Agency heads designated pursuant to Section 1-201 may create special access programs to control access, distribution, and protection of particularly sensitive information classified pursuant to this Order or predecessor orders. Such programs may be created or continued only at the written direction of these agency heads. For special access programs pertaining to intelligence activities (including special activities), or intelligence sources or methods, this function will be exercised by the Director of Central Intelligence. For special access programs pertaining to cryptology, this function will be exercised by the Secretary of Defense.

4-202. Each agency head shall establish and maintain a system of accounting for special access programs. The Director of the Information Security Oversight Office shall have non-delegable access to all such accountings.

4-3. Access by Historical Researchers and Former Presidential Appointees.

4-301. The requirement in Section 4-101 that access to classified information may be granted only as is essential to the accomplishment of authorized and lawful Government purposes may be waived as provided in Section 4-302, for persons who:

(a) are engaged in historical research projects, or

(b) previously have occupied policy-making positions to which they were appointed by the President.

4-302. Waivers under Section 4-301 may be granted only if the agency with jurisdiction over the information:

(a) determines in writing that access is consistent with the interest of national security;

(b) takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with this Order; and

(c) limits the access granted to former presidential appointees to items that the person originated, reviewed, signed or received while serving as a presidential appointee.

SECTION 5. IMPLEMENTATION AND REVIEW.

5-1. Policy Direction.

5-101. The National Security Council shall provide overall policy direction for the information security program.

5-102. The Administrator of General Services shall be responsible for implementing and monitoring the program established pursuant to this Order. This responsibility shall be delegated to the Director of the Information Security Oversight Office.

5-2. Information Security Oversight Office.

5-201. The Information Security Oversight Office shall have a full-time Director appointed by the Administrator of General Services subject to approval by the President. The Director shall have the authority to appoint a staff for the Office.

5-202. The Director shall:

(a) Develop, in consultation with the agencies, and promulgate, subject to the approval of the National Security Council, directives for the implementation of this Order which shall be binding on the agencies;

(b) review all agency implementing regulations and agency guidelines for systematic declassification review. The Director shall require any regulation or guideline to be changed if it is not consistent with this Order or implementing directives. Any such decision by the Director may be appealed to the National Security Council. The agency regulation or guideline shall remain in effect until the appeal is decided;

(c) oversee agency actions to ensure compliance with this Order and implementing directives;

(d) have the authority to conduct on-site reviews of the information security program of each agency that creates or handles classified information and to require of each agency those reports, information, and other cooperation which may be necessary to fulfill the Director's responsibilities. If these reports, inspections, or access to specific categories of classified information would pose an exceptional

national security risk, the affected agency head or the senior official designated under Section 5-301(a) may deny access. The Director may appeal denials to the National Security Council. The denial of access shall remain in effect until the appeal is decided;

(e) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend presidential approval;

(f) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the information security program;

(g) have the authority to prescribe standard forms which will promote the implementation of the information security program;

(h) exercise case-by-case classification authority in accordance with Section 1-205;

(i) report annually to the President through the National Security Council on the implementation of this Order; and

(j) have the authority to convene and chair interagency meetings to discuss matters pertaining to the information security program;

5-3. General Responsibilities.

5-301. Agencies which originate or handle classified information shall:

(a) Designate a senior agency official to direct and administer its information security program, which shall include an active oversight and security education program to ensure effective implementation of this Order;

(b) promulgate implementing regulations. Any unclassified regulations that establish agency information security policy shall be published in the Federal Register to the extent that these regulations affect members of the public; and

(c) establish procedures to prevent unnecessary access to classified information, including procedures which (i) require that a demonstrable need for access to classified information is established before initiating administrative clearance procedures, and (ii) ensure that the number of persons granted access to classified

information is reduced to and maintained at the minimum number that is consistent with operational and security requirements and needs.

5-4. Sanctions.

5-401. If the Director of the Information Security Oversight Office finds that a violation of this Order or its implementing directives may have occurred, the Director shall make a report to the head of the agency or to the senior official designated under Section 5-301(a) so that corrective steps, if appropriate, may be taken.

5-402. Officers and employees of the United States Government shall be subject to appropriate sanctions if they:

(a) knowingly, willfully or negligently disclose without authorization information properly classified under this Order or predecessor orders;

(b) knowingly and willfully classify or continue the classification of information in violation of this Order or any implementing directive; or

(c) knowingly, willfully or negligently violate any other provision of this Order or implementing directive.

5-403. Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, or other sanction in accordance with applicable law and agency regulation.

5-404. Each agency head or the senior official designated under Section 5-301(a) shall ensure that appropriate and prompt corrective action is taken whenever a violation under Section 5-402 occurs. Each shall ensure that the Director of the Information Security Oversight Office is promptly notified whenever a violation under Section 5-402(a) or (b) occurs.

SECTION 6. GENERAL PROVISIONS.

6-1. Definitions.

6-101. "Agency" has the meaning provided at 5 U.S.C. 552(e).

6-102. "Information" includes any information or material, regardless of its physical form or characteristics, that is owned by, produced by, produced for, or is under the control of the United States Government.

6-103. "Classified information" means information that has been determined pursuant to this Order or any predecessor order to require protection against unauthorized disclosure and that is so designated.

6-104. "Foreign government information" means:

(a) Information provided by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, or the source of the information, is to be held in confidence; or

(b) any information produced by the United States pursuant to or as a result of a joint arrangement, with a foreign government or organization of governments, requiring that the information, the arrangement, or both be held in confidence.

6-105. "National security" means the national defense and/or foreign relations of the United States.

6-106. "Confidential source" means any individual or organization which has provided, or which may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the

expectation, expressed or implied, that the information or relationship, or both, be held in confidence.

6-2. General.

6-201. Nothing in this Order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended. "Restricted Data" and "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.

6-202. The Attorney General, upon request by the head of an agency or the Director of the Information Security Oversight Office, shall personally or through authorized representatives of the Department of Justice render an interpretation of this Order with respect to any question arising in the course of its administration.

6-203. Executive Order No. 12065 of June 28, 1978; the accompanying presidential Order of June 28, 1978; Information Security Oversight Office Implementing Directive No. 1 of October 2, 1978; and Section 5-209 of Executive Order No. 12148 of July 20, 1979, are revoked as of the effective date of this Order.

DRAFT

6-204. This Order shall become effective on _____.